AMENDMENTS TO THE CLAIMS

Please **REWRITE** claims 25–26, 32–34, 37, 40–42, 48–50, and 56. For the Examiner's convenience, this Amendment includes the text of all claims under examination, a parenthetical expression for each claim to indicate the status of the claim, and markings to show changes relative to the immediate prior version of each currently amended claim.

1–24. (Canceled).

25. (Currently Amended) A method of determining a public key having an optionally reduced length and a number p for a cryptosystem resident in a device that includes a memory, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising:

selecting a number q and the [[a]] number p such that $p^2 - p + 1$ is an integer multiple of q;

selecting a number g of order q, where g and its conjugates can be represented by B, where

$$F_g(X) = X^3 - BX^2 + B^pX - 1$$ and the roots are g, g^{p^2}, g^{-p}; [[and]]

representing the powers of the conjugates of g using their trace over the field GF(p^2); and

computing the public key as a function of p, q, and B.

26. (Currently Amended) The ~~A method of generating a private key, and computing a public key as a function of p, q, and B generated by the~~ method of claim 25, further comprising: ~~and the private key.~~

generating a private key,

wherein the computing of the public key is a function of p, q, B, and the private key.

27. (Previously Presented) A method of encrypting a message using the public key generated by the method of claim 26.

28. (Previously Presented) A method of decrypting a message using the public key and the private key generated by the method of claim 26.

29. (Previously Presented) A method of signing a message using the public key and the private key generated by the method of claim 26.

30. (Previously Presented) A method of verifying a signature using the public key generated by the method of claim 26.

31. (Previously Presented) A method of key exchange using the public key and the private key generated by the method of claim 26.

32. (Currently Amended) A method of key exchange, such as a Diffie-Hellman key exchange, ~~and related schemes~~ using the public key [[p, q, and B as]] generated by the method of claim 25.

33. (Currently Amended) A system for determining a public key having an optionally reduced length and a number p for a cryptosystem resident in a device that includes a memory, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing

GF(p^6), comprising:

a processor for selecting a number q and the [[a]] number p such that $p^2 - p + 1$ is an integer multiple of q;

said processor selecting a number g of order q, where g and its conjugates can be represented by B, where $F_g(X) = X^3 - BX^2 + B^pX - 1$ and the roots are g, g^{p^2}, g^{-p}; [[and]]

said processor representing the powers of the conjugates of g using their trace over the field GF(p^2); and

said processor computing the public key as a function of p, q, and B.

34. (Currently Amended) The ~~A system of generating a private key, and computing a public key as a function of p, q, and B generated by the~~ system of claim 33, further comprising: ~~and the private key.~~

said processor generating a private key,

wherein the computing of the public key is a function of p, q, B, and the private key.

35. (Previously Presented) A system of encrypting a message using the public key generated by the system of claim 34.

36. (Previously Presented) A system of decrypting a message using the public key and the private key generated by the system of claim 34.

37. (Currently Amended) A system of signing a message using the public key [[ken]] and the

private key generated by the system of claim 34.

38. (Previously Presented) A system of verifying a signature using the public key generated by the system of claim 34.

39. (Previously Presented) A system of key exchange using the public key and the private key generated by the system of claim 34.

40. (Currently Amended) A system of key exchange, such as a Diffie-Hellman key exchange, ~~and related schemes~~ using the public key [[p, q, and B as]] generated by the system of claim 33.

41. (Currently Amended) A computer program article of manufacture for a cryptosystem resident in a device that includes a memory, comprising:

a computer readable medium for determining a public key having an optionally reduced length and a number p, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising:

a computer program means in said computer readable medium, for selecting a number q and the [[a]] number p such that $p^2 - p + 1$ is an integer multiple of q;

a computer program means in said computer readable medium, for selecting a number g of order q, where g and its conjugates can be represented by B, where $F_g(X) = X^3 - BX^2 + B^pX - 1$ and the roots are g, g^{p^1}, g^{-p}; [[and]]

a computer program means in said computer readable medium, for representing the powers

of the conjugates of g using their trace over the field GF(p^2); and

a computer program means in said computer readable medium, for computing the public key as a function of p, q, and B.

42. (Currently Amended) The article of manufacture of claim 41, which further comprises:

a computer program means in said computer readable medium, for generating a private key, wherein the computing of the ~~and computing a~~ public key is [[as]] a function of p, q, [[and]] B, and the private key.

43. (Previously Presented) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for encrypting a message using the public key.

44. (Previously Presented) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for decrypting a message using the public key and the private key.

45. (Previously Presented) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for signing a message using the public key and the private key.

46. (Previously Presented) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for verifying a signature

using the public key.

47. (Previously Presented) The article of manufacture of claim 42, which further comprises:

a computer program means in said computer readable medium, for performing a key exchange using the public key and the private key.

48. (Currently Amended) The article of manufacture of claim 41, which further comprises:

a computer program means in said computer readable medium, for performing a key exchange, such as a Diffie-Hellman key exchange, ~~or a related scheme~~ using the public key [[p, q, and B]].

49. (Currently Amended) A business method of determining a public key having an optionally reduced length and a number p for a cryptosystem resident in a device that includes a memory, using GF(p) or GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6), comprising the steps of:

selecting a number q and the [[a]] number p such that $p^2 - p + 1$ is an integer multiple of q;

selecting a number g of order q, where g and its conjugates can be represented by B, where

$F_g(X) = X^3 - BX^2 + B^pX - 1$ and the roots are g, g^{p^2}, g^{-p}; [[and]]

representing the powers of the conjugates of g using their trace over the field GF(p^2); and

computing the public key as a function of p, q, and B.

50. (Currently Amended) The ~~A method of generating a private key, and computing a public key as a function of p, q, and B generated by the~~ business method of claim 49, further

comprising: ~~and the private key.~~

generating a private key,

wherein the computing of the public key is a function of *p*, *q*, *B*, and the private key.

51. (Previously Presented) A method of encrypting a message using the public key generated by the business method of claim 50.

52. (Previously Presented) A method of decrypting a message using the public key and the private key generated by the business method of claim 50.

53. (Previously Presented) A method of signing a message using the public key and the private key generated by the business method of claim 50.

54. (Previously Presented) A method of verifying a signature using the public key generated by the business method of claim 50.

55. (Previously Presented) A method of key exchange using the public key and the private key generated by the method of claim 50.

56. (Currently Amended) A method of performing a key exchange, such as a Diffie-Hellman key exchange, ~~or a related scheme~~ using the public key [[*p*, *q*, and *B* as]] generated by the business method of claim 49.